RELATIONS D'ÉQUIVALENCE SUR LES ENSEMBLES DE MOTS

par Roland BACHER

RÉSUMÉ. — Le but de cet article est d'étudier une classe de relations d'équivalence sur les monoïdes libres. Ces relations d'équivalence proviennent de l'informatique théorique (systèmes de réécritures) et sont donc également étroitement liées à certaines suites automatiques. Une famille d'exemples particulièrement intéressante est associée à certaines triangulations du plan ainsi qu'à certaines présentations de $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$.

1. Définitions

Notons $\mathcal{A}^*$ le monoïde libre sur un ensemble $\mathcal{A}$ (appelé *alphabet*). Les éléments de $\mathcal{A}^*$ sont donc les mots (associatifs) qu'on peut écrire en n'utilisant que des lettres dans l'alphabet $\mathcal{A}$. On notera $\mathcal{A}^k$ (respectivement $\mathcal{A}^{\leq k}$) le sous-ensemble des mots de longueur k (respectivement de longueur au plus k) dans $\mathcal{A}^*$ et on désignera par $|w| \in \mathbf{N}$ la longueur d'un mot w.

Soit $\mathcal{M}$ un ensemble. Un *graphe* de $\mathcal{M} \times \mathcal{M}$ est un sous-ensemble $G \subset \mathcal{M} \times \mathcal{M}$. Son *graphe réciproque* G^{-1} est défini par $(x,y) \in G^{-1} \iff (y,x) \in G$.

Une *relation d'équivalence* sur $\mathcal{M}$ est un graphe $E \subset \mathcal{M} \times \mathcal{M}$ qui est réflexif ($(w,w) \in E$ pour tout $w \in \mathcal{M}$), symétrique ($(u,v) \in E \Longrightarrow (v,u) \in E$) et transitif ($(u,v),(v,w) \in E \Longrightarrow (u,w) \in E$). Une relation d'équivalence partitionne $\mathcal{M}$ en une réunion disjointe $\mathcal{M} = \bigcup_{C \in \mathcal{C}} C$ de *classes* ou *classes d'équivalence* et permet de définir la fonction $w \longmapsto \mathcal{M}_w$ qui associe à $w \in C = \mathcal{M}_w \subset \mathcal{M}$ sa classe $C = \mathcal{M}_w \in \mathcal{C}$.

1.1. PROPOSITION. — *L'ensemble $\mathcal{C}$ des classes d'équivalence d'une relation d'équivalence E sur $\{0,1,\ldots,q-1\}^*$ est fini si, et seulement si, il existe un entier L tel que tout mot de longueur supérieure à L soit équivalent à un mot strictement plus court.*

Preuve. — Trivial.

Mots-clés : Relation d'équivalence isotrope, relation d'équivalence locale, cône de Farey, SL_2, suite automatique.
Classification math. : 11B85, 68Q42, 69Q68, 68R15.

La relation d'équivalence $E(\mathcal{G})$ engendrée par un ensemble $\mathcal{G} \subset \mathcal{P}(\mathcal{M} \times \mathcal{M})$ de graphes de $\mathcal{M} \times \mathcal{M}$ est par définition le plus petit sous-ensemble réflexif, symétrique et transitif $E(\mathcal{G}) \subset \mathcal{M} \times \mathcal{M}$ avec $\bigcup_{G \in \mathcal{G}} G \subset E(\mathcal{G})$. On écrira souvent $u \sim_{\mathcal{G}} v$ (ou $u \sim v$ quand $\mathcal{G}$ est évident) pour $(u, v) \in E(\mathcal{G})$.

On écrira $E(G)$ si l'ensemble $\mathcal{G}$ est le singleton $\{G\}$ avec $G \subset \mathcal{M} \times \mathcal{M}$.

Une bijection ω d'un monoïde libre $\mathcal{A}^*$ est *isotrope à droite* si elle est de la forme $\omega(xy) = \omega(x)y'$ avec $|\omega(x)| = |x|$ pour tout $x, y \in \mathcal{A}^*$. Notons $\mathcal{BD}$ le groupe formé des bijections isotropes à droite.

On définit également le sous-groupe $\mathcal{BD}^b \subset \mathcal{BD}$ formé des éléments $\omega \in \mathcal{BD}$ pour lesquels il existe $k \in \mathbf{N}$ tel que $\omega(xy) = \omega(x)y$ pour tout $x \in \mathcal{A}^k,\ y \in \mathcal{A}^*$. On notera $|\omega|$ l'entier minimal (appelé *norme* de ω) pour lequel cette condition est satisfaite. On voit aisément qu'on a $|\omega^{-1}| = |\omega|$ et $|\omega \circ \omega'| \leq \max\{|\omega|, |\omega'|\}$ pour $\omega, \omega' \in \mathcal{BD}^b$.

On introduit de même le groupe $\mathcal{BG}$ des isotropies à gauche, son sous-groupe $\mathcal{BG}^b$ ainsi que la fonction norme $\alpha \longmapsto |\alpha|$ sur $\mathcal{BG}^b$. L'application

$$\omega \longmapsto \tau \circ \omega \circ \tau$$

pour $\tau(a_1 a_2 \cdots a_k) = a_k a_{k-1} \cdots a_2 a_1$ avec $a_1, a_2, \ldots, a_k \in \mathcal{A}$, induit un isomorphisme entre les groupes $\mathcal{BD}$ et $\mathcal{BG}$ ainsi qu'entre leurs sous-groupes $\mathcal{BD}^b$ et $\mathcal{BG}^b$.

Un graphe $G \subset \mathcal{A}^* \times \mathcal{A}^*$ est *isotrope* s'il existe $u, v \in \mathcal{A}^*,\ \alpha \in \mathcal{BG}$ et $\omega \in \mathcal{BD}$ tels que

$$G = \left\{ (xuy, \alpha(x)v\omega(y)) \mid x, y \in \mathcal{A}^* \right\}.$$

Son graphe réciproque G^{-1} est alors donné par

$$G^{-1} = \left\{ (xvy, \alpha^{-1}(x)u\omega^{-1}(y)) \mid x, y \in \mathcal{A}^* \right\}.$$

Un tel graphe est *local* si $\alpha \in \mathcal{BG}^b$ et $\omega \in \mathcal{BD}^b$.

1.2. Définition. — Une relation d'équivalence sur $\mathcal{A}^*$ est *isotrope* (respectivement *locale*) si elle est engendrée par un ensemble (ou une réunion) de graphes isotropes (respectivement locaux) de $\mathcal{A}^* \times \mathcal{A}^*$.

Les relations d'équivalence locales qui n'admettent qu'un nombre fini de classes constituent le principal objet d'étude de ce papier. De telles relations d'équivalence sont étroitement liées à certains systèmes de réécriture (voir [E] ou [Ho]). Une grande partie du contenu des sections 1 et 2 est donc probablement bien connue en informatique théorique.

1.3. Exemple. — Considérons sur le monoïde $\{0,1\}^*$ un graphe local $G \subset \{0,1\}^* \times \{0,1\}^*$ de la forme

$$G = \left\{ (x0y, \alpha(x)\omega(y)) \mid x, y \in \{0,1\}^* \right\}$$

tel qu'il existe deux entiers $a, b,\ a+b > \min(|\alpha|, |\omega|)$ vérifiant $\alpha(1^a) = 0u,\ \omega(1^b) = v0$ où 1^k désigne le mot bègue constant $11\cdots11$ de longueur k. On a donc $u \in \{0,1\}^{a-1}$ et $v \in \{0,1\}^{b-1}$.

Déterminons pour la relation d'équivalence locale $E(G)$les mots de $\{0,1\}^*$ qui sont de longueur minimale dans leur classe.

Tout mot $w \in \{0,1\}^*$ contenant la lettre 0 est équivalent à un mot plus court.

Sous l'hypothèse $|\alpha| < a+b$ (l'argument pour $|\omega| < a+b$ est analogue) on a pour $x, y \in \{0,1\}^*$:

$$x1^a1^by \sim x'0u0v0y' \sim x'0\alpha(u0v)\omega(y') \sim \alpha(x')\omega(\alpha(u0v)\omega(y'))$$

avec $x' \in \{0,1\}^{|x|}, y' \in \{0,1\}^{|y|}$ convenables. Tout mot contenant le facteur (sous-mot formé de lettres consécutives) bègue constant 1^k de longueur $k \geq a+b$ est donc équivalent à un mot plus court dans $\{0,1\}^*$.

Les seuls mots qui ne possèdent pas forcément un représentant plus court dans leur classe appartiennent donc à l'ensemble $\{\emptyset, 1, 11, \ldots, 1^{a+b-1}\}$ et $\{0,1\}^*$ contient donc au plus $a+b$ classes d'équivalence.

La section 3 contient une description élémentaire de l'exemple associé à $|\alpha| = a = |\omega| = b = 1$. Ses sous-sections 3a et 3b en décrivent un peu plus finement quelques propriétés.

1.4. Exemple. — Soit S un semi-groupe de présentation finie $\langle G, R\rangle$ avec ensemble générateur F et ensemble de relations R. L'ensemble des éléments de S est alors l'ensemble des classes d'équivalence d'une relation locale sur F^* qui est engendrée par les graphes locaux

$$\{(xr_1y, xr_2y) \mid x, y \in F^*\}$$

pour $r_1 = r_2$ relation dans R.

En particulier, tout sous-ensemble générateur F d'un groupe fini G fournit une relation d'équivalence locale avec un nombre fini de classes d'équivalence sur F^*.

1.5. Plan du papier. — La section 2 énonce quelques résultats généraux.

La section 3 et ses sous-sections 3a et 3b contiennent une étude plus approfondie d'un exemple de relation d'équivalence locale sur $\{0,1\}^*$ (voir Exemple 1.3 ci-dessus). Elles ne dépendent aucunement des autres sections et elles peuvent être lues isolément.

La section 4 décrit une construction géométrique d'une relation d'équivalence locale sur $\{0,\ldots,q-1\}^*$. Cette construction généralise l'exemple étudié dans la section 3 (qui est le cas $q = 2$ de cette construction).

La section 5 montre que la théorie des relations d'équivalence locales sur $\{0,\dots,q-1\}^*$ est contenue dans la théorie des q-automates.

La section 6 introduit les relations d'équivalence locales pour les mots cycliques.

2. Résultats généraux

2.1. Définition. — Soit $\mathcal{A}$ un alphabet. Un graphe $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ est *finitaire* si $\widetilde{G}$ est réunion finie de graphes isotropes et $\widetilde{G}$ vérifie les deux conditions suivantes :

(i) $(x,y) \in \widetilde{G} \Rightarrow |x| \geq |y|$,

(ii) Il existe un entier L tel que pour tout mot w de longueur supérieure à L on peut trouver un mot r_w strictement plus court avec $(w, r_w) \in \widetilde{G}$.

L'intérêt des graphes finitaires provient principalement de "l'algorithme" suivant (que j'appelle pseudo-algorithme car il n'est pas bien déterminé ; une variante déterministe est facile à concevoir mais aura moins d'intérêt théorique) :

2.2. Pseudo-algorithme (associé à un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$). — Donnée initiale : $w \in \mathcal{A}^*$.

(i) Si

$$\{w\} \times \mathcal{A}^{<|w|} \cap \widetilde{G} = \emptyset\ ,$$

afficher w et terminer.

(ii) Choisir $r_w \in \mathcal{A}^*$ avec $|r_w| < |w|$ et $(w, r_w) \in \widetilde{G}$, remplacer w par r_w (une telle substitution est une *réduction élémentaire associée à* $\widetilde{G}$) et revenir à *(i)*.

Ce processus termine après un nombre fini d'itérations car la longueur du mot w diminue strictement à chaque itération.

Notons $R_{\widetilde{G}}(w) \subset \mathcal{A}^*$ l'ensemble des résultats (appelés *réduites de* w) qu'on peut obtenir à partir de la donnée initiale $w \in \mathcal{A}^*$. On a évidemment $(w,r) \in E(\widetilde{G})$ pour toute réduite $r \in R_{\widetilde{G}}(w)$ de w.

La condition *(ii)* de la définition 2.1 montre que l'ensemble $\mathcal{R}_{\widetilde{G}} = \bigcup_{w \in \mathcal{A}^*} R_{\widetilde{G}}(w)$ de toutes les réduites est un sous-ensemble de $\mathcal{A}^{\leq L}$.

2.3. Proposition. — *Une relation d'équivalence isotrope E sur $\mathcal{A}^* = \{0,\dots,q-1\}^*$ est engendrée par un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ si, et seulement si, E ne possède qu'un nombre fini de classes d'équivalence.*

2.4. Lemme. — *Soit* $G = \{((xuy), \alpha(x)v\omega(y)) \mid x, y \in \mathcal{A}^*\}$ *un graphe isotrope de* $\mathcal{A}^* \times \mathcal{A}^*$. *Pour* $\tilde{x}, \tilde{y} \in \mathcal{A}^*$ *définissons* $\alpha_{\tilde{x}} \in \mathcal{BG}, \omega_{\tilde{y}} \in \mathcal{BD}$ *par* $\alpha_{\tilde{x}}(x)\alpha(\tilde{x}) = \alpha(x\tilde{x}),\ \omega(\tilde{y})\omega_{\tilde{y}}(y) = \omega(\tilde{y}y)$.

(i) L'ensemble $G' = \{(x(\tilde{x}u\tilde{y})y, \alpha_{\tilde{x}}(x)(\alpha(\tilde{x})v\omega(\tilde{y}))\omega_{\tilde{y}}(y)) \mid x, y \in \mathcal{A}^*\}$ *est un sous-graphe isotrope de* G.

(ii) Si G *est local, alors* $|\alpha_{\tilde{x}}| \leq \max(0, |\alpha| - |\tilde{x}|)$ *et* $|\omega_{\tilde{y}}| \leq \max(0, |\omega| - |\tilde{y}|)$.

Preuve. — On a par définition de $\alpha_{\tilde{x}}$ et de $\omega_{\tilde{y}}$:

$$\alpha_{\tilde{x}}(x)\alpha(\tilde{x})v\omega(\tilde{y})\omega_{\tilde{y}}(y) = \alpha(x\tilde{x})v\omega(\tilde{y}y)$$

ce qui montre que

$$G' = \{(x\tilde{x}u\tilde{y}y, \alpha(x\tilde{x})v\omega(\tilde{y}y)) \mid x, y \in \mathcal{A}^*\} \subset G\,.$$

L'assertion *(ii)* est évidente. ∎

2.5. Lemme. — *Soit* E *une relation d'équivalence isotrope sur* $\mathcal{A}^*$. *Alors* $(u, v) \in E$ *si, et seulement si, il existe* $\alpha_{u,v} \in \mathcal{BG},\ \omega_{u,v} \in \mathcal{BD}$ *tels que*

$$G_{u,v} = \{(xuy, \alpha_{u,v}(x)v\omega_{u,v}(y)) \mid x, y \in \mathcal{A}^*\} \subset E\,.$$

Preuve. — Ceci résulte du fait que $G \subset E \iff G^{-1} \subset E$ et du lemme précédent.

Preuve de la proposition 2.3. — Si $\widetilde{G}$ est un graphe finitaire, toute classe d'équivalence C de $E(\widetilde{G})$ possède un représentant dans l'ensemble fini $\mathcal{A}^{\leq L}$ avec $L \in \mathbf{N}$ comme dans la définition 2.1.

Considérons maintenant une relation d'équivalence isotrope E qui n'admet qu'un nombre fini de classes sur $\mathcal{A}^* = \{0, \ldots, q-1\}^*$. Soit L un entier tel que toute classe possède un représentant de longueur au plus L. Tout mot $w \in \mathcal{A}^{L+1}$ est alors équivalent à un mot r_w de longueur $\leq L$. Le lemme 2.4 montre donc qu'il existe un graphe isotrope G_{w,r_w} qui est de la forme

$$G_{w,r_w} = \{(xwy, \alpha_w(x)r_w\omega_w(y)) \mid x, y \in \mathcal{A}^*\} \subset E\,.$$

Le graphe $\widetilde{G} = \bigcup_{w \in \mathcal{A}^{L+1}} G_{w,r_w}$ est alors finitaire et on a l'inclusion $E(\widetilde{G}) \subset E$. Comme $E(\widetilde{G})$ ne possède qu'un nombre fini de classes d'équivalence, on peut (en utilisant le lemme 2.5) obtenir l'égalité après adjonction d'un nombre fini de sous-graphes isotropes de E. ∎

Soit $E(\widetilde{G})$ une relation d'équivalence sur $\mathcal{A}^* = \{0, \ldots, q-1\}^*$ qui est engendrée par un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$.

Considérons pour $n \in \mathbf{N}$ la relation d'équivalence $\widetilde{E}(\widetilde{G}, n)$ engendrée par

$$\left\{(x, y) \in \mathcal{A}^{\leq n} \times \mathcal{A}^{\leq n} \mid (x, y) \in \widetilde{G}\right\}$$

sur $\mathcal{A}^{\leq n}$.

La relation $\widetilde{E}(\widetilde{G}, n)$ sur $\mathcal{A}^{\leq n}$ est alors plus fine que la restriction de la relation $E(\widetilde{G})$ à $\mathcal{A}^{\leq n}$ (*i.e.* on a $(x, y) \in \widetilde{E}(\widetilde{G}, n) \Rightarrow (x, y) \in E(\widetilde{G})$).

2.6. Théorème. — *Soit $\mathcal{A}^*$ un monoïde libre sur un alphabet fini $\mathcal{A}$. Soit $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ un graphe finitaire.*

Alors il existe un entier N tel que la relation d'équivalence $\widetilde{E}(\widetilde{G}, n)$ sur $\mathcal{A}^{\leq n}$ coïncide avec la restriction de la relation d'équivalence $E(\widetilde{G})$ à $\mathcal{A}^{\leq n}$ pour tout entier $n \geq N$.

Preuve. — Une inspection du pseudo-algorithme 2.2 montre que tout mot w de longueur supérieure à L admet une réduite $r_w \in \mathcal{A}^{\leq L}$ telle que $(w, r_w) \in \widetilde{E}(\widetilde{G}, |w|) \subset E(\widetilde{G})$.

Il suffit donc de montrer que les restrictions de $E(\widetilde{G})$ et $\widetilde{E}(\widetilde{G}, n)$ coïncident sur l'ensemble fini des réduites $\mathcal{R}_{\widetilde{G}} = \bigcup_{w \in \mathcal{A}^*} R_{\widetilde{G}}(w)$.

Deux réduites $(r, r') \in E(\widetilde{G}) \cap R_{\widetilde{G}} \times R_{\widetilde{G}}$ peuvent être jointes par une chaîne finie $w_0 = r, w_1, \ldots, w_\ell = r'$ de mots telle que $(w_{i-1}, w_i) \in \widetilde{G} \cup \widetilde{G}^{-1}$ pour $i = 1, \ldots, \ell$. Il existe donc $N_{r,r'} \in \mathbf{N}$ tel que $|w_i| \leq N_{r,r'}$ pour $i = 0, \ldots, \ell$ et on a donc également $(r, r') \in \widetilde{E}(\widetilde{G}, N_{r,r'})$.

Les deux relations d'équivalence coïncident donc sur $\mathcal{A}^{\leq n}$ si

$$n \geq N = \max_{r,r' \in \mathcal{R}, (r,r') \in E(\widetilde{G})} \left\{N_{r,r'}\right\}.$$

2.7. Proposition. — *Soit $\widetilde{G} = \bigcup_{j=1}^{s} G_j \subset \mathcal{A}^* \times \mathcal{A}^*$ un graphe finitaire avec $G_j = \left\{(x u_j y, \alpha_j(x) v_j \omega_j(y))\right\} \subset \mathcal{A}^* \times \mathcal{A}^*$ des graphes locaux pour $j = 1, \ldots, s$. Soit $L = L(\widetilde{G})$ comme dans la définition 2.1.*

Alors la valeur

$$N = 2 \max_j\{|u_j|\} + 3L + \max_j\{|\alpha_j| + |\omega_j|\} + \max_j\{|\alpha_j|\} + \max_j\{|\omega_j|\} + 1$$

convient pour le théorème 2.6.

Preuve. — Soit $w_1 \sim w_2 \sim w_3$ un bout de chaîne comme dans la preuve du théorème 2.6 et supposons $|w_2| \geq N$. On peut alors trouver une chaîne $w_1 \sim w_1' \sim w_2' \sim w_3' \sim w_3$ telle que $|w_i'| < |w_i|$ pour $i = 1, 2, 3$.

En effet, supposons d'abord w_2 de la forme

$$w_2 = xa_1u_1b_1ya_2u_2b_2z$$

où $w_1 = x\alpha(a_1)r_1\omega(b_1)ya_2u_2b_2z$ et $w_3 = xa_1u_1b_1y\alpha(a_2)r_2\omega(b_2)z$. Les hypothèses montrent alors qu'on a, ou bien $|xa_1| > L + \max(|\omega_i|)$, ou bien $|b_2z| > L + \max(|\alpha_i|)$, ou bien $|b_1ya_2| > L + \max(|\alpha_i| + |\omega_i|)$. Un de ces bouts (au moins) peut donc être raccourci avant de passer par w_2 (et re-allongé ensuite).

Le cas où les deux réductions liant w_2 à w_1 et w_3 "se chevauchent" laisse encore plus de place pour ce raccourcissement.

Une itération de ce procédé montre donc que deux mots équivalents w et w' de longueur $\leq N$ peuvent être joints par une chaîne d'éléments de longueur au plus N. ∎

2.8. Remarque. — Un analogue de la proposition 2.7 pour les graphes finitaires isotropes (mais non locaux) n'existe pas. Ceci implique que les relations d'équivalence associées ne peuvent pas être étudiées algorithmiquement.

Soit $E \subset \mathcal{A}^* \times \mathcal{A}^*$ le graphe d'une relation d'équivalence locale. Considérons le graphe $E_p \subset \mathcal{A}^* \times \mathcal{A}^*$ défini par

$$(u,v) \in E_p \Longleftrightarrow (xuy, xvy) \in E \text{ pour tout } x,y \in \mathcal{A}^* .$$

2.9. Proposition.

(i) E_p est une relation d'équivalence locale (appelée la relation d'équivalence locale propre associée à E) qui est plus fine que E (i.e. $(a,b) \in E_p \Rightarrow (a,b) \in E$).

(ii) Le nombre de classes d'équivalence d'une relation d'équivalence E sur $\mathcal{A}^* = \{0,\dots,q-1\}^*$ est fini si, et seulement si, le nombre de classes de E_p est fini.

(iii) L'ensemble $\mathcal{C}_p$ des classes d'équivalence d'une relation d'équivalence locale propre E_p est un monoïde (i.e. un ensemble muni d'une loi de composition associative ainsi que d'un élément neutre e à gauche et à droite pour cette loi de composition) pour la loi de composition donnée par la concaténation de représentants. L'élément neutre est représenté par la classe d'équivalence du mot vide $\emptyset$.

Preuve. — L'assertion *(i)* est évidente.

Pour montrer l'assertion *(ii)*, il suffit de remarquer que $(u,v) \in E \Rightarrow (xuy, xvy) \in E_p$ pour tout $x,y \in \mathcal{A}^*$ avec $|x| \geq \max_i |\alpha_i|$, $|y| \geq \max_i |\omega_i|$ où la relation d'équivalence locale E est engendrée par un ensemble fini de graphes locaux

$$\left\{ (x, u_iy, \alpha_i(x)v_i\omega_i(y)) \mid x,y \in \mathcal{A}^* \right\} .$$

L'assertion *(iii)* est évidente. ∎

Remarquons que le semi-groupe $\mathcal{C}_p$ introduit par l'assertion *(iii)* ci-dessus est fini si, et seulement si, E où E_p ne possède qu'un nombre fini de classes d'équivalence. Dans ce cas, pour que $\mathcal{C}_p$ soit un groupe, il faut et il suffit que les représentants des classes de $0, 1, \ldots, q-1$ soient d'ordre fini dans le semi-groupe $\mathcal{C}_p$.

Remarquons encore que l'assertion *(iii)* de la proposition 2.9 permet également la construction d'un anneau $K[\mathcal{C}_p]$ pour tout anneau commutatif K. La construction est la même que pour l'algèbre de groupe d'un groupe.

3. La relation locale $\cdots ab \cdots \sim \cdots (a+1)0(b+1)\cdots$ sur $\{0,1\}^*$

Soit $\{0,1\}$ l'alphabet dont les lettres 0 et 1 forment le corps à deux éléments. On considère sur l'ensemble $\{0,1\}^*$ des mots en 0 et 1 la relation d'équivalence engendrée par

$$x_1 \cdots x_k \sim 0(x_1+1)x_2x_3 \cdots x_k \sim x_1 \cdots (x_i+1)0(x_{i+1}+1)\cdots x_k \sim x_1x_2 \cdots x_{k-1}(x_k+1)0$$

pour $i = 1, \ldots, k-1$ où $x_1, \ldots, x_k \in \{0,1\}$ et $k \in \mathbf{N}$.

Par la suite on utilisera la notation condensée

$$\cdots ab \cdots \sim \cdots (a+1)0(b+1)\cdots$$

où $a, b \in \{0, 1, \emptyset\}$ et $x \longmapsto (x+1)$ est défini par $(0+1) = 1$, $(1+1) = 0$, $(\emptyset+1) = \emptyset$. La notation $\cdots az$ pour $a \in \{0, 1, \emptyset\}$ désigne un mot $w \in \{0,1\}^*$ de la forme $w = xaz$ (avec $x \in \{0,1\}^*$) si $a \neq \emptyset$ et $w = z$ si $a = \emptyset$. Les conventions sont analogues pour $zb\cdots$

3.1. Théorème. — *Cette relation d'équivalence partitionne les éléments de* $\{0,1\}^*$ *en deux classes non-équivalentes représentées par le mot vide* $\emptyset$ *et par le mot* 1.

Pour la preuve de ce théorème il est utile de considérer le pseudo-algorithme suivant ("pseudo" car nécessitant des choix).

3.2. Pseudo-algorithme. — *Donnée initiale :* $w \in \{0,1\}^*$.

(i) Si $w = \emptyset$ *ou* $w = 1$ *afficher* w *et terminer.*

(ii) Choisir une des substitutions (appelées réductions*) possibles parmi*

$$\begin{array}{lll} R_1 : & xa0by \longmapsto x(a+1)(b+1)y & x, y \in \{0,1\}^*,\ a, b \in \{0, 1, \emptyset\} \\ R_2 : & x11y \longmapsto xy & x, y \in \{0,1\}^* \end{array}$$

(comme plus haut : $a = \emptyset$ *entraîne* $x = \emptyset$ *; idem pour b), l'effectuer sur* w *et revenir à (i).*

Ce pseudo-algorithme effectue au plus $|w|$ itérations (où $|w| \in \mathbf{N}$ désigne la longueur du mot w) car les deux réductions R_1 et R_2 remplacent w par un mot strictement plus court.

Montrons que le résultat final appartient à $\{\emptyset, 1\}$. En effet, si $w = 0$ on peut lui appliquer la réduction R_1 avec $x = y = a = b = \emptyset$ pour obtenir $\emptyset$. Si la longueur de w est au moins 2, alors w contient, ou bien une lettre 0 et peut être raccourci par une réduction du type R_1, ou bien w est de la forme $w = x11y$ et admet donc une réduction du type R_2. Dans les deux cas on obtient un mot strictement plus court et seuls les mots $\emptyset$ et 1 ne peuvent plus être réduits.

On dira que le pseudo-algorithme 3.2 est *défini pour* $w \in \{0,1\}^*$ si le résultat final ($\in \{\emptyset, 1\}$) est indépendant des choix effectués lors des itérations de *(ii)*. Le pseudo-algorithme 3.2 est *défini* s'il l'est pour tout mot $w \in \{0,1\}^*$.

Preuve du théorème 3.1. — On a clairement $w \sim r_w$ pour $w, r_w \in \{0,1\}^*$ reliés par une réduction R_1.

Le calcul

$$\cdots a11b\cdots \sim \cdots a000b\cdots \sim \cdots (a+1)10b\cdots \sim \cdots (a+1)0(b+1)\cdots \sim \cdots ab\cdots$$

montre qu'on a également $w \sim r_w$ pour r_w obtenu en appliquant une réduction du type R_2 à w.

Le pseudo-algorithme construit donc un mot $\bar{r} \in \{\emptyset, 1\}$ avec $\bar{r} \sim w$. Il existe donc au plus deux classes d'équivalence distinctes.

Pour prouver que $\emptyset \not\sim 1$, il suffit de montrer que le pseudo-algorithme 3.2 est défini.

En effet, si $\emptyset \sim 1$, il existe une suite finie de mots

$$w_0 = \emptyset, w_1 = 0, w_2, w_3, \ldots, w_{\ell-1} = 00, w_\ell = 1$$

de $\{0,1\}^*$ telle que

$$\{w_{i-1}, w_i\} = \{\cdots ab\ldots\ ,\ \ldots (a+1)0(b+1)\cdots\},$$

c'est-à-dire deux mots consécutifs $w_{i-1},\ w_i$ sont reliés par une réduction du type R_1. Comme le pseudo-algorithme est clairement défini et diffère sur $w_0 = \emptyset$ et sur $w_\ell = 1$, il ne peut pas être défini pour tout mot w_j de la chaîne.

Soit $w \in \{0,1\}^*$ un mot de longueur minimale pour lequel le pseudo-algorithme n'est pas défini. Le mot w admet donc deux premières réductions ρ et ρ' (du type R_1 ou R_2) qui se prolongent chacune en une suite de réductions (des types R_1 et R_2) aboutissant respectivement à $\emptyset$ et à 1.

Comme w est de longueur minimale pour cette propriété, on doit avoir $\rho \neq \rho'$ car autrement on peut remplacer w par le mot $\rho(w)$ qui est plus court.

Appelons *support* d'une réduction de type R_1 ou R_2 les 3 ou 2 lettres concernées par la réduction.

Les supports de ρ et ρ' s'intersectent : en effet, si les supports de ρ et ρ' ne s'intersectent pas, on peut considérer le mot $\rho(\rho'(w)) = \rho'(\rho(w))$. Par minimalité de w, le pseudo-algorithme est bien défini et fournit donc le même résultat pour les mots $\rho(\rho'(w))$, $\rho(w)$ et $\rho'(w)$ qui sont strictement plus courts que w.

Si ρ et ρ' sont deux réductions du type R_2, il n'y a rien a vérifier car, ou bien elles possèdent des supports distincts, ou bien elles sont associées à un sous-mot de la forme 111 et on a alors $\rho(w) = \rho'(w)$.

Si ρ est de type R_2 et ρ' de type R_1, on peut supposer (quitte à remplacer $w = x_1 \dots x_k$ par son miroir $\tau(w) = x_k x_{k-1} \cdots x_2 x_1$) qu'on a $w = \cdots 110a \cdots$ avec $a \in \{0, 1, \emptyset\}$. On a alors d'une part

$$\cdots \underline{11}0a \cdots \mapsto \cdots 0a \cdots$$

et d'autre part

$$\cdots 1\underline{10a} \cdots \mapsto \cdots \underline{10(a+1)} \cdots \mapsto \cdots 0a \cdots$$

ce qui montre l'égalité dans ce cas (les lettres soulignées indiquent les supports des réductions effectuées).

Si les deux réductions sont du type R_1, on peut supposer qu'elles sont centrées en deux coefficients 0 adjacents (car autrement $\rho(\rho'(w)) = \rho'(\rho(w)$ et on conclut comme plus haut).

On a donc $w = \cdots a00x$ où $a \in \{\emptyset, 0, 1\}$ et $x \in \{0, 1\}^*$. Quitte à prendre le miroir, on peut également supposer $x \neq \emptyset$ car le pseudo-algorithme 3.2 est défini pour le mot 00.

Pour $w = \cdots a000b \cdots$ avec $b \in \{0, 1, \emptyset\}$ on obtient

$$\cdots \underline{a00}0b \cdots \mapsto \cdots (a+1)\underline{10b} \cdots \mapsto \cdots \underline{(a+1)0(b+1)} \cdots \mapsto \cdots ab \cdots$$

d'une part et

$$\cdots a\underline{000}b \cdots \mapsto a\underline{11}b \cdots \mapsto ab \cdots$$

d'autre part.

Pour $w = \cdots a001b \cdots$ on a

$$\cdots \underline{a00}1b \cdots \mapsto \cdots (a+1)\underline{11}b \cdots \mapsto \cdots (a+1)b \cdots$$

et

$$\cdots a\underline{001}b \cdots \mapsto \cdots a\underline{10b} \cdots \mapsto \cdots \underline{a0(b+1)} \cdots \mapsto \cdots (a+1)b \cdots$$

ce qui termine la preuve. ∎

On verra également une preuve "géométrique" du théorème 3.1 dans la section 4.

Pour $w \in \{0,1\}^*$, notons $\{0,1\}^*_w \subset \{0,1\}^*$ l'ensemble des mots équivalents à w et $\{0,1\}^k_w = \{0,1\}^*_w \cap \{0,1\}^k$ l'ensemble des mots de longueur k dans $\{0,1\}^*_w$.

Les deux tables suivantes contiennent tous les mots dans $\{0,1\}^k_\emptyset$ et $\{0,1\}^k_1$ pour $k \leq 5$.

3.3. TABLE DES MOTS DE LONGUEUR ≤ 5 DANS $\{0,1\}_\emptyset$.

$$\begin{aligned}
\{0,1\}^0_\emptyset &= \{\emptyset\}\\
\{0,1\}^1_\emptyset &= \{0\}\\
\{0,1\}^2_\emptyset &= \{01,\ 10,\ 11\}\\
\{0,1\}^3_\emptyset &= \{000,\ 001,\ 011,\ 100,\ 110\}\\
\{0,1\}^4_\emptyset &= \{0000,\ 0010,\ 0100,\ 0101,\ 0111,\ 1001,\ 1010,\ 1011,\ 1101,\ 1110,\ 1111\}\\
\{0,1\}^5_\emptyset &= \{00001,\ 00010, 00011,\ 00101,\ 00110,\ 00111,\ 01000, 01010,\ 01100,\ 01101,\\
&\quad 01111,\ 10000,\ 10001, 10011,\ 10100,\ 10110,\ 11000,\ 11001,\ 11011,\ 11100,\ 11110\}
\end{aligned}$$

3.4. TABLE DES MOTS DE LONGUEUR ≤ 5 DANS $\{0,1\}_1$.

$$\begin{aligned}
\{0,1\}^1_1 &= \{1\}\\
\{0,1\}^2_1 &= \{00\}\\
\{0,1\}^3_1 &= \{010,\ 101,\ 111\}\\
\{0,1\}^4_1 &= \{0001,\ 0011,\ 0110,\ 1000,\ 1100\}\\
\{0,1\}^5_1 &= \{00000,\ 00100,\ 01001,\ 01011,\ 01110,\ 10010,\ 10101,\ 10111,\ 11010,\ 11101,\\
&\quad 11111\}
\end{aligned}$$

3.5. REMARQUE. — On peut également considérer la relation d'équivalence $\sim_p$ (voir aussi la proposition 2.9) sur $\{0,1\}^*$ engendrée par

$$\cdots 11 \cdots \sim_p \cdots \emptyset \cdots$$

et

$$\cdots a0b \cdots \sim_p \cdots (a+1)(b+1) \cdots$$

pour $a, b \in \{0,1\}$ (mais $a = \emptyset$ ou $b = \emptyset$ exclu).

Le lecteur pourra aisément vérifier que les classes d'équivalence de $\sim_p$ sur $\{0,1\}^*$ forment le groupe $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ (qui est isomorphe au groupe dihédral à 6 éléments ou encore au groupe symétrique Sym_3 des permutations de 3 objets) en prenant la concaténation de représentants de classes comme loi de groupe.

Un tel isomorphisme est par exemple donné par

$$\begin{array}{llll} \emptyset & \mapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \qquad 0 \quad \mapsto \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad 1 \quad \mapsto \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 00 & \mapsto & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & \qquad 01 \quad \mapsto \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad 10 \quad \mapsto \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \end{array}$$

La relation d'équivalence $\sim_p$ est évidemment plus fine que la relation d'équivalence $\sim$ introduite précédemment. Plus précisément, la classe de $\emptyset$ pour $\sim$ est la réunion des classes $\emptyset$, 0, 01 et 10 pour $\sim_p$. Les deux classes restantes (1 et 00) de $\sim_p$ forment la classe de 1 pour $\sim$.

Dans la suite, la sous-section 3a est consacrée à l'étude de quelques propriétés arithmétiques des ensembles $\{0,1\}^*_\emptyset$ et $\{0,1\}^*_1$ (pour la relation d'équivalence $\sim$ considérée avant la remarque 3.5).

Dans la sous-section 3b, on établira un lien avec les mots cycliques.

3a. Arithmétique.

Dans cette sous-section ainsi que dans la sous-section 3b, la relation d'équivalence $\sim$ considérée sera toujours la relation d'équivalence sur $\{0,1\}^*$ engendrée par

$$\cdots a0b\cdots \sim \cdots (a+1)(b+1)\cdots$$

avec $a, b \in \{0,1,\emptyset\}$ et $(0+1)=1$, $(1+1)=0$ et $(\emptyset+1)=\emptyset$.

3a.1. Proposition.

(i) Si $w \sim w' \sim 1$ *alors* $ww' \sim \emptyset$ *et* $w0w' \sim w1w' \sim 1$.

(ii) Si $w \sim 1$ *et* $w' \sim \emptyset$ *alors* $w0w' \sim w1w' \sim w'0w \sim w'1w \sim \emptyset$.

Preuve. — Si les mots $w, w' \in \{0,1\}^*_1$ sont de longueur >1 on peut les réduire en évitant des réductions du type $R_1 : \cdots a0b\cdots \longmapsto \cdots (a+1)(b+1)\cdots$ centrées en une lettre 0 à la fin du mot w ou au début du mot w'. Ces réductions sont compatibles avec la concaténation des mots. On peut donc supposer $w = w' = 1$ et la preuve de *(i)* résulte d'une inspection des tables 3.3 et 3.4.

Pour montrer que $w\epsilon w' \sim \emptyset$ (avec $\epsilon \in \{0,1\}$) dans le cas *(ii)* on procède de manière analogue. On peut donc supposer $w = 1$. Le mot w' appartient après réduction à l'ensemble $\{\emptyset, 0, 01\}$ et une inspection de la table 3.3 permet de conclure. La preuve pour $w'\epsilon w \sim \emptyset$ est analogue. ∎

On peut également démontrer la proposition 3a.1 (ainsi que beaucoup d'autres résultats dans la suite) en utilisant la relation $\sim_p$ (qui est plus fine que $\sim$) introduite dans la

remarque 3.5. On est alors ramené à vérifier un certain nombre d'identités dans le groupe $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$.

3a.2. Corollaire (Factorisation des mots dans $\{0,1\}_1^*$). — *Un mot $w \in \{0,1\}^*$ est équivalent à 1 si, et seulement si, il est de la forme*

$$w = f_1\epsilon_1 f_2\epsilon_2 \cdots f_{k-1}\epsilon_{k-1}f_k$$

où $\epsilon_1, \ldots, \epsilon_{k-1} \in \{0,1\}$ et $f_1, \ldots, f_k \in \{1,\ 00,\ 010,\ 0110,\ 01110,\ \ldots,\ 011\cdots110,\ \ldots\}$ et cette factorisation est unique.

Preuve. — Un calcul simple donne l'inclusion

$$\{1, 00, 010, 0110, 01110, 011110, 0111110, \ldots\} \subset \{0,1\}_1^*$$

et une récurrence utilisant l'assertion *(i)* de la proposition 3a.1 montre que tout mot w de la forme

$$w = f_1\epsilon_1 \cdots f_{k-1}\epsilon_{k-1}f_k$$

avec $\epsilon_i \in \{0,1\}$ et $f_i \in \{1, 00, 010, 0110, \ldots\}$, appartient à $\{0,1\}_1^*$.

D'autre part, il est facile de vérifier que les mots $\{1, 00, 010, 0110, \ldots\} \subset \{0,1\}_1^*$ sont les seuls mots de la forme $w = x_1x_2\cdots x_k$ tels que $x_1x_2\cdots x_j \in \{0,1\}_\emptyset^*$ pour tout $j < k$. Cette remarque et la proposition 3a.1 impliquent alors l'existence d'une factorisation $w = f_1\epsilon_1 \cdots f_{k-1}\epsilon_{k-1}f_k$ pour $w \in \{0,1\}_1^*$. Nous laissons la preuve de son unicité au lecteur. ∎

Pour $w, x \in \{0,1\}^*$ notons $\{0,1\}_w^*x$ l'ensemble des mots obtenus en concaténant un mot dans $\{0,1\}_w^*$ avec x. Pour K un anneau et E un ensemble, notons $K[E]$ le K-module libre sur E.

3a.3. Corollaire. — *Soit K un anneau.*

(i) Les K-modules $K[\{0,1\}_1^*0]$, $K[\{0,1\}_1^*1]$ et $K[\{0,1\}_1^*0 \cup \{0,1\}_1^*1]$ sont des anneaux (le produit est la concaténation des mots).

(ii) Le K-module $K[\{0,1\}_\emptyset^*]$ est un module à gauche pour ces structures d'anneaux.

Preuve. — Ceci résulte immédiatement de la proposition 3a.1.

3a.4. Remarque. — Les structures d'anneaux définies par le corollaire 3a.3 peuvent être prolongées en des structures d'algèbres de Hopf après adjonction d'une unité (qu'on peut représenter par $\emptyset$).

En effet, un mot $w \in \{0,1\}_1^* 1$ s'écrit de manière unique sous la forme

$$w = h_1 1 h_2 1 \cdots h_k 1$$

avec $h_i = f_{i_1} 0 f_{i_2} 0 \cdots f_{i_\ell - 1} 0 f_{i_\ell}$ où $f_{i_j} \in \{1, 00, 010, 0110, \ldots\}$. On obtient alors un coproduit sur $K[\{0,1\}_1^* 1 \cup \{\emptyset\}]$ en posant $\Delta(\emptyset) = \emptyset \otimes \emptyset$ et

$$\Delta(w) = \sum_{J \subset \{1,\ldots,k\}} \Big(\prod_{i \in J} h_i 1 \Big) \otimes \Big(\prod_{j \notin J} h_j 1 \Big) .$$

L'antipode est donné par $\iota(w) = (-1)^k h_k 1 h_{k-1} 1 \cdots h_2 1 h_1 1$.

La structure d'algèbre de Hopf sur $K[\{0,1\}_1^* 0 \cup \{\emptyset\}]$ est analogue.

La structure d'algèbre de Hopf sur $K[\{0,1\}_1^* 0 \cup \{0,1\}_1^* 1 \cup \{\emptyset\}]$ est donnée par le coproduit : $\Delta(\emptyset) = \emptyset \otimes \emptyset$ et

$$\Delta(w) = \sum_{J \subset \{1,\ldots,k\}} \Big(\prod_{i \in J} f_i \epsilon_i \Big) \otimes \Big(\prod_{j \notin J} f_j \epsilon_j \Big)$$

où $w = f_1 \epsilon_1 f_2 \epsilon_2 \cdots f_k \epsilon_k \in \{0,1\}_1^* 0 \cup \{0,1\}_1^* 1$.

Antipode : $\iota(w) = (-1)^k f_k \epsilon_k f_{k-1} \epsilon_{k-1} \cdots f_2 \epsilon_2 f_1 \epsilon_1$.

Les algèbres de Hopf ainsi obtenues sont isomorphes à une algèbre de Hopf bien connue associée au monoïde libre sur un alphabet infini (appelée spray-concatenation Hopf algebra dans [H]).

3a.5. Proposition.

(i) Pour tout mot w équivalent à $\emptyset$ il existe un unique $\alpha, \beta \in \{0,1\}$ tels que $\alpha w \sim w\beta \sim 1$,

(ii) On a pour tout $w \sim 1$

$$0w \sim 1w \sim w0 \sim w1 \sim \emptyset .$$

(iii) On a pour tour tout mot $w = au = vb \in \{0,1\}_1^k$ (avec $a, b \in \{0,1\}$ convenables)

$$u \sim v \sim \emptyset .$$

Preuve. — Le même raisonnement qu'au début de la preuve de la proposition 3a.1 montre qu'on peut supposer w de longueur au plus 2. Une inspection de la table 3.4 montre alors *(i)*.

Pour montrer *(ii)*, il suffit de considérer le cas où $w = 1$.

Pour prouver l'assertion *(iii)* on se ramène au cas où le mot w est de longueur au plus 3 et on termine par une inspection des tables 3.3 et 3.4. ∎

3a.6. Corollaire. — *On a*

$$|\{0,1\}^k_\emptyset| = \frac{2^{k+1}+(-1)^k}{3} \qquad , \qquad |\{0,1\}^k_1| = \frac{2^k-(-1)^k}{3}$$

(où $\{0,1\}^k_w$ désigne l'ensemble fini des mots de longueurs k qui sont équivalents à w).

Preuve. — Les assertions *(iii)* et *(i)* de la proposition 3a.5 montrent qu'on a $|\{0,1\}^k_1| = |\{0,1\}^{k-1}_\emptyset|$ pour $k \geq 1$ et on termine par une récurrence sur k. ∎

3a.7. Remarque. — On peut également compter les mots de $\{0,1\}^{n+1}_1$ en utilisant la "factorisation" des mots dans $\{0,1\}^*_1$ décrite par le corollaire 3a.2. On obtient ainsi l'identité

$$\sum_k \binom{n-k}{k} 2^k = \frac{2^{n+1}+(-1)^n}{3}\,.$$

Cette identité se généralise en considérant d'autres sous-ensembles de $\{0,1\}^*$ (ou d'un monoïde sur un alphabet plus grand) qui ont des propriétés de factorisation analogues. Ainsi en posant

$$f_n = \sum_k \binom{n-k}{k}$$

on obtient la suite de Fibonacci : $f_0 = f_1 = 1$ et $f_n = f_{n-1} + f_{n-2}$ $(n \geq 2)$.

3b. Structures cycliques.

Soit $E \subset \{0,1\}^k$ un ensemble de mots de même longueur k. On associe à E un graphe orienté $\Gamma(E)$ de sommets E comme suit :

Deux mots $w, w' \in E$ sont reliés par une arête orientée de w à w' si, et seulement si, il existe $\tilde{w} \in \{0,1\}^{k-1}$ et $\alpha, \beta \in \{0,1\}$ tels que

$$w = \tilde{w}\beta \qquad \text{et} \qquad w' = \alpha\tilde{w}\,.$$

On appellera w' un *successeur* de w et w un *prédécesseur* de w'.

3b.1. Proposition. — *Le graphe $\Gamma(\{0,1\}^k_1)$ associé à l'ensemble $\{0,1\}^k_1 \subset \{0,1\}^*_1$ de mots de longueur k qui sont équivalents à 1 est une réunion de cycles orientés.*

Preuve. — Les assertions *(i)* et *(iii)* de la proposition 3a.5 montrent que tout mot $w \in \{0,1\}^*_1$ possède un unique successeur et un unique prédécesseur. Ceci implique que le graphe $\Gamma(\{0,1\}^k_1)$ est une réunion de cycles orientés dans l'ensemble fini $\{0,1\}^k_1$. ∎

3b.2. Proposition. — *Soit $w = \alpha\tilde{w}$, $w' = \tilde{w}\beta \in \{0,1\}^k_1$ avec $\alpha, \beta \in \{0,1\}$ deux mots équivalents à 1 qui se succèdent.*

Considérons le mot infini $(k+1)$-périodique $W = \cdots \alpha\tilde{w}\beta\alpha\tilde{w}\beta\alpha\tilde{w}\beta\cdots = \overline{\alpha\tilde{w}\beta}$. On a alors :

(i) Tous les k-facteurs (sous-mots formés de k lettres consécutives) de W sont dans $\{0,1\}_1^k$,

(ii) Tous les facteurs de longueur $k \pm 1$ du mot W sont dans $\{0,1\}_\emptyset^*$.

Preuve. — Soit u un k-facteur de W. Si $u = \alpha\tilde{w}$ ou $u = \tilde{w}\beta$ alors $u \in \{0,1\}_1^k$ par hypothèse. On peut donc supposer $u = \tilde{u}_2\beta\alpha\tilde{u}_1$ où $\tilde{w} = \tilde{u}_1\epsilon\tilde{u}_2$ pour $\epsilon \in \{0,1\}$ convenable. Si u est de longueur > 6, alors au moins un des deux mots $\tilde{u}_2\beta$, $\alpha\tilde{u}_1$ est de longueur > 3 et on peut lui appliquer une réduction dont le support ne le dépasse pas. Ceci montre qu'il suffit de vérifier l'assertion *(i)* pour tous les mots de longueur au plus 6 dans $\{0,1\}_1^*$. Une inspection de la table 3.4 et un petit calcul permettent de conclure.

L'assertion *(ii)* résulte de *(i)* et des assertions *(ii)* et *(iii)* de la proposition 3a.5. ∎

3b.3. Corollaire.

(i) Les longueurs des cycles du graphe $\Gamma(\{0,1\}_1^k)$ divisent tous $k+1$.

(ii) Les composantes connexes (les cycles distincts) de $\Gamma(\{0,1\}_1^k)$ sont en bijection avec les mots binaires périodiques dont tous les facteurs de longueur k sont équivalents à 1.

Preuve. — L'assertion *(i)* résulte de la proposition 3b.2 car la période minimale du mot périodique $W = \overline{\alpha\tilde{w}\beta}$ défini dans la proposition 3b.2 est un diviseur de $k+1$.

L'assertion *(ii)* est évidente. ∎

3b.4. Table. — Cycles des graphes $\Gamma(\{0,1\}_1^k)$ pour $k = 1,\ldots,7$.

(Les mots périodiques $\overline{x_1x_2x_3\cdots x_{k-1}x_k}$ et $\overline{x_2x_3\cdots x_{k-1}x_kx_1}$ sont évidemment identiques.)

$\{0,1\}_1^1 : \overline{1}$

$\{0,1\}_1^2 : \overline{0}$

$\{0,1\}_1^3 : \overline{01}, \overline{1}$

$\{0,1\}_1^4 : \overline{01100}$

$\{0,1\}_1^5 : \overline{011101}, \overline{001}, \overline{0}, \overline{1}$

$\{0,1\}_1^6 : \overline{0111100}, \overline{0000101}, \overline{0011011}$

$\{0,1\}_1^7 : \overline{01111101}, \overline{00000011}, \overline{00101101}, \overline{00100111}, \overline{0001}, \overline{0111}, \overline{01}, \overline{1}$.

3b.5. Proposition.

(i) Soit W un mot périodique dont tous les k-facteurs appartiennent à $\{0,1\}_1^k$. Alors tous les facteurs de longueur $\lambda(k+1)-1$ de W appartiennent également à $\{0,1\}_1^*$ pour $\lambda = 1,2,3,4\ldots$

(ii) Tout mot périodique W admet une longueur primitive $\mathrm{lp}(W) \in \mathbf{N}$, i.e. il existe un entier $k = \mathrm{lp}(W)$ tel que tout k-facteur de W est équivalent à 1 et tout entier $k' \in \mathbf{N}$ avec la même propriété est de la forme $k' = \lambda(k+1)-1$ pour $\lambda \in \{1,2,\ldots\}$). Cette longueur primitive appartient à l'ensemble $\{p-1, 2p-1, 3p-1\}$ pour W périodique de période minimale p.

Preuve.

(i) est une conséquence facile de l'assertion *(i)* de la proposition 3a.1.

Pour montrer *(ii)* commençons par montrer que toute suite périodique $W = \overline{x_1 x_2 \cdots x_p}$ de période minimale p admet un entier $k \in \{p-1, 2p-1, 3p-1\}$ avec la propriété que tout k-facteur de W appartient à $\{0,1\}_1^*$.

Une petite vérification (voir table 3b.6 ci-dessous) montre que si W est de période minimale $p \leq 3$ il existe un tel entier $k \in \{2p-1, 3p-1\}$. On peut donc supposer $W = \overline{x_1 x_2 \cdots x_p}$ de période minimale $p \geq 4$. Considérons les deux coefficients x_2 et x_3 de W. Si $x_2 x_3 = 11$ posons $W' = \overline{x_1 x_4 x_5 \cdots x_p}$. Pour $x_2 = 0$, posons $W' = \overline{(x_1+1)(x_3+1)x_4 \cdots x_p}$, pour $x_2 x_3 = 10$ posons $W' = \overline{x_1 0 (x_4+1) x_5 \cdots x_p}$. Le mot périodique $W' = \overline{x'_1 x'_2 \cdots x'_{p'}}$ possède donc une période $p' < p$. Par hypothèse de récurrence, il existe $k' \in \{p'-1, 2p'-1, 3p'-1\}$ tel que tout k'-facteur de W' appartient à $\{0,1\}_1^{k'}$. En particulier, les deux k'-facteurs commençant par $x'_1 x'_2 \cdots$ et $x'_2 x'_3 \cdots$ appartiennent à $\{0,1\}_1^{k'}$. Posons $k = \mu p - 1$ avec $\mu = (k'+1)/p' \in \{1,2,3\}$. Les deux k-facteurs consécutifs w_1 et w_2 de W commençant par $x_1 x_2 \cdots$ et $x_2 x_3 \cdots$ appartiennent alors également à $\{0,1\}_1^k$. La proposition 3b.2 montre l'appartenance à $\{0,1\}_1^k$ de tous les k-facteurs du mot $(k+1)$-périodique $\tilde{W}$ associé et on a $\tilde{W} = W$.

Démontrons maintenant l'existence d'une longueur primitive pour un mot périodique W de période minimale p.

Considérons l'entier minimal $k \geq 1$ pour lequel tout k-facteur de W appartient à $\{0,1\}_1^k$. L'assertion *(i)* du corollaire 3b.3 montre que k est de la forme $k = \mu p - 1$ avec μ un entier strictement positif et on vient de voir que μ appartient à l'ensemble $\{1,2,3\}$.

Si $\mu = 1$, il n'y a rien à démontrer à cause de l'assertion *(i)* ci-dessus. L'entier $k = p-1$ est la longueur primitive de W.

Considérons maintenant les cas $\mu = 2$ ou $\mu = 3$ et supposons qu'il existe un entier k' tel que tout k'-facteur de W soit dans $\{0,1\}_1^{k'}$ avec $k' \neq \lambda\mu p - 1$ pour λ entier. Comme on a $k' = \lambda' p - 1$, il existe $\tilde{\lambda}$ tel que $|\tilde{\lambda}\mu - \lambda'| = 1$ (car $\mu = 2$ ou $\mu = 3$). Posons $\tilde{k} = \tilde{\lambda}\mu p - 1$. On a donc $|\tilde{k} - k'| = p$ et tous les facteurs de longueur $\tilde{k}$ et k' de W sont dans $\{0,1\}_1^*$. La proposition 3a.1 implique alors que tous les facteurs de longueur $p-1$ de W appartiennent également à $\{0,1\}_1^*$ ce qui contredit la minimalité de $k = \mu p - 1$. ∎

3b.6. Table. — Longueurs primitives $\mathrm{lp}(W)$ des mots périodiques W de période minimale ≤ 5 :

$$\begin{aligned}
&\mathrm{lp}(\overline{0}) = 2\,,\\
&\mathrm{lp}(\overline{1}) = 1\,,\\
&\mathrm{lp}(\overline{01}) = 3\,,\\
&\mathrm{lp}(\overline{001}) = 5\,,\\
&\mathrm{lp}(\overline{011}) = 8\,,\\
&\mathrm{lp}(\overline{0001}) = 7\,,\\
&\mathrm{lp}(\overline{0011}) = 11\,,\\
&\mathrm{lp}(\overline{0111}) = 7\,,\\
&\mathrm{lp}(\overline{00001}) = 9\,,\\
&\mathrm{lp}(\overline{00011}) = 4\,,\\
&\mathrm{lp}(\overline{00101}) = 14\,,\\
&\mathrm{lp}(\overline{00111}) = 9\,,\\
&\mathrm{lp}(\overline{01011}) = 9\,,\\
&\mathrm{lp}(\overline{01111}) = 14\,.
\end{aligned}$$

3b.7. Remarque. — Étant donnée une suite périodique $W = \overline{x_1 \cdots x_p}$ de période primitive p et un entier $\ell \geq 1$, on peut définir une nouvelle suite p-périodique $\tau_\ell(W) = \overline{z_1 z_2 \cdots z_p}$ en posant $z_i = 0$ si le facteur $x_i x_{i+1} \cdots$ de longueur ℓ dans W appartient à $\{0,1\}_\emptyset^\ell$. On posera $z_i = 1$ sinon. La proposition 3b.2 montre alors qu'ou bien $\tau_{\ell p-1}(W) = \overline{1}$ (si μ divise ℓ où $\mu p - 1$ est la longueur primitive de W) ou bien deux lettres adjacentes de $\tau_{\ell p-1}(W)$ ne sont jamais toutes les deux égales à 1. La proposition 3b.5 peut alors se reformuler comme suit : ou bien $\tau_{p-1}(W) = \overline{1}$ (cas $\mathrm{lp}(W) = p - 1$) et $\tau_\ell(W)$ ne dépend que de $\ell \pmod p$ ou bien $\tau_{p-1}(W) \neq \tau_{2p-1}(W) = \overline{1}$ et $\tau_\ell(W)$ ne dépend que $\ell \pmod{2p}$ (cas $\mathrm{lp}(W) = 2p - 1$) ou bien $\tau_{p-1}(W), \tau_{2p-1}(W) \neq \tau_{3p-1}(W) = \overline{1}$ et $\tau_\ell(W)$ ne dépend que de $\ell \pmod{3p}$ (cas $\mathrm{lp}(W) = 3p - 1$).

Soit $w' = \tilde{w}b \in \{0,1\}_1^*$ le successeur du mot $w = a\tilde{w} \in \{0,1\}_1^*$. On définit les applications successeur et prédécesseur $\sigma, \sigma^{-1} : \{0,1\}_1^* \longrightarrow \{0,1\}$ par

$$\begin{aligned}
&\sigma(w) = \sigma(a\tilde{w}) = b\,,\\
&\sigma^{-1}(w') = \sigma^{-1}(\tilde{w}b) = a\,.
\end{aligned}$$

3b.8. Proposition. — *Les applications successeur et prédécesseur $w \longmapsto \sigma(w)$,*

$\sigma^{-1}(w) \in \{0,1\}$ sont données par

$$\sigma(f_1\epsilon_1\cdots f_j\epsilon_j f_{j+1}) = \sigma^{-1}(f_1\epsilon_1\cdots f_j\epsilon_j f_{j+1}) = (\sum_{i=1}^{j}\epsilon_i) + (\sum_{i=1}^{j+1}|f_i|) \pmod 2$$

où $|w|$ désigne la longueur d'un mot w et où $f_1\epsilon_1\cdots f_j\epsilon_j f_{j+1}$ est la "factorisation" d'un mot dans $\{0,1\}_1^*$ décrite au corollaire 3a.2.

Preuve. — On peut réduire les facteurs "premiers" $f_i \in \{1, 00, 010, 0110, \ldots\}$ qui sont de longueur > 3 par une réduction de type R_2 ($x11y \longmapsto xy$) et cette réduction est compatible avec la formule à démontrer. On peut donc supposer $f_1, \ldots, f_{j+1} \in \{1, 00, 010\}$.

On démontre ensuite la formule pour $\sigma(w)$ par récurrence sur j. La preuve pour $j = 0$ résulte d'une inspection de la table 3.4.

Il suffit ensuite de considérer les 18 choix possibles pour $f_1, f_2 \in \{1, 00, 010\}$ et pour $\epsilon_1 \in \{0,1\}$. Un petit calcul laissé au lecteur montre que toutes ces possibilités peuvent se réduire (en évitant les réductions de type R_1 centrée en la dernière lettre) à des cas plus simples (avec un nombre $j' < j$ de "facteurs premiers") de manière compatible avec la formule à démontrer.

La formule pour σ^{-1} se démontre de façon analogue. On peut également utiliser la proposition 3b.2 qui implique directement l'égalité $\sigma^{-1}(w) = \sigma(w)$ pour tout $w \in \{0,1\}_1^*$. ∎

4. Cônes de Farey et SL_2

4.1. Définition. — Une *suite de Farey généralisée* est une suite finie de nombres rationnels

$$\frac{p_0}{q_0} = \frac{0}{1}, \frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k} = \frac{1}{1}$$

avec $p_i, q_i \geq 0$ entiers telle que $p_i q_{i+1} - p_{i+1} q_i = -1$ pour $i = 0, \ldots, k-1$.

En particulier, les entiers p_i, q_i sont premiers entre eux et on peut considérer la suite

$$(p_0, q_0) = (0,1), \ldots, (p_k, q_k) = (1,1)$$

de points dans $\mathbf{Z}^2$.

4.2. Définition. — Un *cône de Farey* est une suite finie de longueur au moins 2 de la forme

$$(p_0, q_0) = (0,1), \ldots, (p_k, q_k)$$

dans $\mathbf{Z}^2$ telle que $p_i q_{i+1} - p_{i+1} q_i = -1$ pour $i = 0, \ldots, k-1$.

Un *cône de Farey affine* est une orbite d'un cône de Farey sous l'action du groupe $\mathrm{Aff}^+(\mathbf{Z}^2)$ où $\mathrm{Aff}^+(\mathbf{Z}^2)$ est le groupe formé de toutes les transformations affines qui préservent l'orientation et le réseau affine $\mathbf{Z}^2$ des points entiers dans $\mathbf{R}^2$.

Un cône de Farey se représente géométriquement par un ensemble de triangles de sommets entiers $(p_i, q_i), (p_{i+1}, q_{i+1})$ et $(0,0)$ et d'aire $1/2$ qu'on recolle deux à deux. On obtient de cette sorte une espèce d'éventail qui fait d'abord ℓ fois le tour de l'origine (dans le sens des aiguilles d'une montre) et qui s'arrête finalement contre la demi-droite issue de $(0,0)$ et passant par (p_k, q_k).

On appellera le nombre $2\ell\pi + \mathrm{angle}((0,1),(p_k,q_k))$ l'*angle* du cône de Farey où $\mathrm{angle}((0,1),(p_k,q_k)) \in [0, 2\pi)$ désigne l'angle (non orienté) évident entre les deux vecteurs $(0,1)$ et (p_k, q_k).

Soit C un cône de Farey affine représenté par un cône de Farey $(p_0,q_0) = (0,1), \ldots, (p_k,q_k)$. On vérifie facilement que le nombre ℓ de tours complets du représentant ainsi que l'entier p_k et la classe de $q_k \pmod{p_k}$ sont indépendants du représentant. On appellera le triplet $(2\ell\pi, p_k, q_k \pmod{p_k})$ l'*angle affine* de C et on utilisera les conventions (naturelles) que l'angle est $2\ell\pi$ si $(p_k,q_k) = (0,1)$, il est $(2\ell+1)\pi$ si $(p_k,q_k) = (0,-1)$ (où ℓ est le nombre de tours complets) et l'angle $(2\ell\pi, -p_k, q_k \pmod{p_k})$ est identifiée à l'angle $((2\ell+1)\pi, p_k, -q_k \pmod{p_k})$ si $p_k > 0$.

4.3. Lemme. — *La suite*

$$(p_0,q_0) = (0,1), \ldots, (p_i,q_i), (p_{i+1},q_{i+1}), \ldots, (p_k,q_k)$$

est un cône de Farey si, et seulement si, la suite

$$(p_0,q_0) = (0,1), \ldots, (p_i,q_i), (p_i+p_{i+1}, q_i+q_{i+1}), (p_{i+1},q_{i+1}), \ldots, (p_k,q_k)$$

est un cône de Farey.

La preuve est une vérification facile.

On dira que deux cônes de Farey (affines) sont reliés par un *mouvement élémentaire* s'ils sont comme dans le lemme 4.3 (s'ils possèdent des représentants comme dans le lemme 4.3). Le premier cône de Farey (affine) est alors une *réduction élémentaire* du deuxième.

4.4. Théorème.

(i) Si l'angle d'un cône de Farey est $< \pi$ alors le cône C se transforme par un nombre fini de réductions élémentaires en un unique cône de Farey $\widetilde{C}$ (ayant même angle) qui est

minimale, i.e. les points de $\widetilde{C}$ forment une sous-suite de points de C' pour tout cône de Farey C' ayant même angle que $\widetilde{C}$.

(i') L'analogue de l'assertion (i) reste vraie pour les cônes de Farey affines ayant un angle affine de la forme $(0, p_k, q_k \pmod{p_k})$ avec $p_k > 0$.

(ii) Un cône de Farey (affine) C peut être transformé en un cône de Farey (affine) C' par un nombre fini de mouvements élémentaires si, et seulement si, C et C' ont même angle (affine).

Ce théorème se prouve par des considérations géométriques. Nous laissons les détails au lecteur.

Soit $\lambda = (\lambda_1, \ldots, \lambda_k) \in \mathbf{Z}^k$ une suite d'entiers de longueur k. Considérons la suite $CF(\lambda) \subset \mathbf{Z}^2$ formée des $k+2$ points suivants :

$$(p_0, q_0) = (0,1),\ (p_1, q_1) = (1,0) \quad \text{et} \quad (p_{i+1}, q_{i+1}) = -(p_{i-1}, q_{i-1}) - (\lambda_i - 1)(p_i, q_i)$$

ou, en écriture matricielle,

$$\begin{pmatrix} p_{i+1} & p_i \\ q_{i+1} & q_i \end{pmatrix} = \begin{pmatrix} 1-\lambda_1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1-\lambda_2 & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1-\lambda_i & 1 \\ -1 & 0 \end{pmatrix}.$$

4.5. Proposition. — *L'application $\lambda \longmapsto CF(\lambda)$ est une bijection entre l'ensemble des suites entières de longueur finie et l'ensemble des cônes de Farey affines.*

4.6. Proposition. — *Un cône de Farey affine $CF(\mu)$ avec $\mu = (\mu_1, \ldots, \mu_k)$ est une réduction élémentaire d'un cône de Farey affine $CF(\lambda)$ si, et seulement si,*

$$\lambda = (\mu_1, \ldots, \mu_{i-2}, (\mu_{i-1} - 1), 0, (\mu_i - 1), \mu_{i+1}, \ldots, \mu_k)$$

pour un indice $i \in \{1, \ldots, k+1\}$ (avec les conventions $\lambda = (0, (\mu_1 - 1), \mu_2, \ldots, \mu_k)$ respectivement $\lambda = (\mu_1, \ldots, \mu_{k-1}, (\mu_k - 1), 0)$ si $i = 1$ respectivement $i = k+1$).

Les preuves des propositions 4.5 et 4.6 sont faciles et laissées au lecteur.

Considérons sur l'ensemble $\mathbf{Z}^*$ des suites finies à valeurs entières la relation d'équivalence engendrée par

$$\lambda_1, \ldots, \lambda_{i-1}, 0, \lambda_i, \ldots, \lambda_k \sim \lambda_1, \ldots, (\lambda_{i-1} + 1), (\lambda_i + 1), \ldots, \lambda_k$$

(*i.e.* engendrée par des suites correspondantes à des cônes de Farey affines reliés par un mouvement élémentaire) en utilisant les mêmes conventions que dans la proposition 4.6.

4.7. Corollaire. — *Deux suites finies d'entiers λ et μ sont dans la même classe d'équivalence si, et seulement si, les cônes de Farey affines associés $CF(\lambda)$ et $CF(\mu)$ ont même angle affine.*

Preuve. — Cela résulte des propositions 4.5, 4.6 et du théorème 4.4. ∎

4.8. Remarque. — Ce corollaire permet d'obtenir une présentation (qui n'est cependant pas de type fini) du groupe $\tilde{\mathrm{SL}}_2(\mathbf{Z}) \subset \tilde{\mathrm{SL}}_2(\mathrm{R})$ où $\pi : \tilde{\mathrm{SL}}_2(\mathrm{R}) \longrightarrow \mathrm{SL}_2(\mathrm{R})$ est le revêtement universel de $\mathrm{SL}_2(\mathrm{R})$ et où $\tilde{\mathrm{SL}}_2(\mathbf{Z}) = \pi^{-1}(\mathrm{SL}_2(\mathbf{Z}))$.

Un élément de $\tilde{\mathrm{SL}}_2(\mathbf{Z})$ peut alors être représenté par une suite $\tilde{\lambda} = (\tilde{\lambda}_1, \ldots, \tilde{\lambda}_k)$ avec $\tilde{\lambda}_i \in \{\ldots, -2_\pm, -1_\pm, 0_\pm, 1_\pm, 2_\pm, \ldots\}$ et les relations sont engendrées par $\tilde{a}_+\tilde{a}_-$, $\tilde{a}_-\tilde{a}_+$, $(a+1)_\epsilon(b+1)_\epsilon = a_\epsilon 0_\epsilon b_\epsilon$ et $(a+k)_+(b+k)_- = a_+b_-$, $(a+k)_-(b+k)_+ = a_-b_+$ pour $a, b, k \in \mathbf{Z}$ et $\epsilon \in \{+,-\}$. Géométriquement, on peut interpréter une telle suite $\tilde{\lambda}$ comme une espèce de cône replié et l'angle (convenablement défini) d'un tel objet est bien sûr relié au fait que le revêtement $\pi : \tilde{\mathrm{SL}}_2(\mathrm{R}) \longrightarrow \mathrm{SL}_2(\mathrm{R})$ est cyclique infini.

Pour obtenir $\mathrm{SL}_2(\mathbf{Z})$ (respectivement $\mathrm{PSL}_2(\mathbf{Z})$), il suffit de rajouter la relation $1_+1_+1_+1_+$ (respectivement 1_+1_+). Plus précisément, un homomorphisme de $(\mathbf{Z}_\pm)^*/\langle\text{relations}\rangle$ dans $\mathrm{SL}_2(\mathbf{Z})$ est donnée par

$$a_+ \longmapsto \begin{pmatrix} 1-a_+ & 1 \\ -1 & 0 \end{pmatrix}, \; a_- \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 1-a_- \end{pmatrix}.$$

Le résultat suivant résume quelques calculs utiles pour la suite.

4.9. Proposition.

(i) On a pour tous $a, b \in \{\emptyset\} \cup \mathbf{Z}$ et pour tout entier n :

$$\cdots a1nb\cdots \sim \cdots (a+n)2(b+1)\cdots$$
$$\cdots an1b\cdots \sim \cdots (a+1)2(b+n)\cdots$$

(où $x \longmapsto (x+1)$ est défini par $(x+1) = x+1$ si $x \in \mathbf{Z}$ et $(x+1) = \emptyset$ si $x = \emptyset$).

(ii) On a également

$$\cdots a2nb\cdots \sim \cdots (a-1)n2(b+1)\cdots .$$

Preuve. — Pour $n = 0$ les formules *(i)* sont vraies par définition de $\sim$. Le calcul

$$\cdots a1(n+1)b\cdots \sim \cdots a00nb\cdots \sim \cdots (a+1)1nb\cdots \sim (a+1+n)2(b+1)\cdots$$

montre par récurrence que la première des formules *(i)* est vraie pour $n \geq 0$ et le calcul

$$\cdots a1(n-1)b\cdots \sim \cdots (a-1)00(n-1)b\cdots$$
$$\sim \cdots (a-1)1nb\cdots \sim \cdots (a-1+n)2(b+1)\cdots$$

montre qu'il en est de même pour $n \leq 0$.

La deuxième formule *(i)* se démontre en regardant ce qui précède dans un miroir.

Pour démontrer *(ii)* on note qu'on a

$$\cdots a2nb\cdots \sim \cdots (a-1)01nb\cdots \sim \cdots (a-1)n2(b+1)\cdots ,$$

l'équivalence des deux derniers membres résultant de l'assertion *(i)* ci-dessus. ∎

Un *cône de Farey modulo q* est une suite

$$(p_0,q_0)=(0,1),\ldots,(p_k,q_k)$$

de points dans $(\mathbf{Z}/q\mathbf{Z})^2$ telle que $p_iq_{i+1}-p_{i+1}q_i=-1 \pmod q$.

Un *cône de Farey affine modulo q* est défini de la manière évidente (en remplaçant le groupe $\mathrm{Aff}^+(\mathbf{Z}^2)$ par le produit semi-direct de $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$ avec $(\mathbf{Z}/q\mathbf{Z})^2$).

L'angle d'un tel cône affine est un élément de la forme (h,r) avec $h\in\mathbf{Z}/q\mathbf{Z}$ et $r\in\mathbf{Z}/q\mathbf{Z} \pmod h$ tel que h et un relevé de r engendrent $\mathbf{Z}/q\mathbf{Z}$.

Pour $q=\prod_{p\text{ premier}} p^{\nu_p}$, un petit calcul montre qu'il existe $\prod_p(2p^{\nu_p}-p^{\nu_p-1}-1)$ possibilités pour l'angle d'un tel cône affine.

La version correspondante de la proposition 4.5 reste valable pour les cônes de Farey affines modulo q et implique facilement les résultats suivants.

4.10. Théorème.

(i) La relation d'équivalence sur $\{0,\ldots,q-1\}^*$ engendrée par $\lambda\sim_{\mathrm{aa}}\mu$ si, et seulement si, les cônes de Farey affines $CF(\lambda)$ et $CF(\mu)$ modulo q associés ont même angle, est une relation d'équivalence locale.

(ii) Le semi-groupe $\mathcal{C}_p$ formé des classes d'équivalence de la relation d'équivalence locale propre $\sim_{\mathrm{aa}\,p}$ associée à la relation $\sim_{\mathrm{aa}}$ ci-dessus, est le groupe $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$. Le rajout de la relation $11\sim_{\mathrm{aa}\,p}\emptyset$ fournit $\mathrm{PSL}_2(\mathbf{Z}/q\mathbf{Z})$.

Introduisons comme ci-dessus la relation d'équivalence engendrée par

$$\cdots a0b\cdots \sim \cdots (a+1)(b+1)\cdots$$

sur $\{0,\ldots,q-1\}^*$ (avec les conventions évidentes pour $x\longmapsto(x+1)$).

4.11. Proposition. — *Si deux suites finies λ et μ sont dans la même classe d'équivalence (pour $\sim$), alors les cônes de Farey affines modulo q associés ont même angle affine.*

Cette proposition dit que la relation d'équivalence engendrée par $\cdots a0b\cdots\sim\cdots(a+1)(b+1)\cdots$ sur $\{0,\ldots,q-1\}^*$ est plus fine que la relation d'équivalence $\lambda\sim_{\mathrm{aa}}\mu\iff CF(\lambda)$ et $CF(\mu)$ ont même angle affine.

4.12. Théorème. — *Pour $q=2$ et $q=3$, ces deux relations d'équivalence coïncident.*

Pour $q = 2$, il existe deux classes (pour ces relations d'équivalence) représentées par $\emptyset$ et 1.

Pour $q = 3$, il existe quatre classes représentées par $\emptyset, 1, 2$ et 22.

Preuve. — Pour $q = 2$ la relation d'équivalence engendrée par $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ possède au plus deux classes représentées par $\emptyset$ et 1 (cf. début de la section 3). Comme il existe également deux possibilités pour l'angle affine d'une cône affine modulo 2, on doit avoir exactement deux classes.

Pour $q = 3$, considérons un représentant $w \in \{0,1,2\}^*$ de longueur minimale d'une classe d'équivalence dans la relation engendrée par $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ La définition de la relation d'équivalence montre que w ne contient pas de 0. Si w contient un 1 et est de longueur au moins 2, on peut le raccourcir à l'aide de l'assertion *(i)* de la proposition 4.9. Si le mot w ne contient que des 2 et est de longueur au moins 3, on peut le transformer en un mot de même longueur qui contient ou bien 0 ou bien 1 en utilisant l'assertion *(ii)* de la proposition 4.9.

Ceci montre que w appartient à l'ensemble $\{\emptyset, 1, 2, 22\}$.

D'autre part, l'angle affine d'un cône de Farey affine modulo 3 prend exactement 4 valeurs distinctes. ∎

4.13. Remarque. — Pour $q = 4$ la relation d'équivalence $\sim$ engendrée par $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ sur $(\mathbf{Z}/4\mathbf{Z})^*$ possède au plus 9 classes qui intersectent toutes l'ensemble $\{\emptyset, 1, 2, 3, 22, 23 \sim 32, 33, 232 \sim 323, 333\}$.

J'ignore si pour d'autres valeurs de q (≥ 5) le nombre de classes de la relation d'équivalence engendrée par $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ est fini. Si c'est le cas, on obtient ainsi une relation d'équivalence locale et on peut se demander si cette relation d'équivalence locale coïncide avec la relation d'équivalence locale donnée par le théorème 4.10.

Je termine cette section par un problème de théorie des groupes.

Pour $s \in \{0, \ldots, q-1\}$ notons $\nu(s) \geq 1$ l'ordre de la matrice

$$\begin{pmatrix} 1-s & 1 \\ -1 & 0 \end{pmatrix}$$

dans $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$.

Considérons la relation d'équivalence locale $\sim'$ sur $\{0, \ldots, q-1\}^*$ engendrée par la relation d'équivalence locale propre associée à $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ (pour $a, b \in \{0, \ldots, q-1, \emptyset\}$) et par les relations locales $\cdots s^{\nu(s)}\cdots \sim' \cdots\emptyset\cdots$ pour $s = 0, \ldots, q-1$.

Alors les classes d'équivalence $\mathcal{C}'$ de $\sim'$ forment un groupe qui possède $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$ comme quotient.

4.14. Problème. — Comprendre ce groupe. Pour quelles valeurs de q obtient-on directement $\mathrm{SL}_2(\mathbf{Z}/q\mathbf{Z})$ (c'est le cas pour $q = 2, 3$)? Pour quelles valeurs de q est-il fini?

5. Suites automatiques

5.1. Définition. — Un *q-automate* (déterministe) Γ (pour $q \geq 1$ entier) (ou un automate complet dans le langage de [E]) est la donnée d'un ensemble fini $S(\Gamma)$ (dont les éléments sont les *sommets* ou les *états* de l'automate) ainsi que d'un ensemble $\varphi_0, \varphi_1, \ldots, \varphi_{q-1} : S(\Gamma) \longrightarrow S(\Gamma)$ de fonctions avec la propriété qu'il existe parmi les états $S(\Gamma)$ un *état initial* marqué $*$ avec $\varphi_0(*) = *$.

On peut représenter graphiquement un tel automate Γ en choisissant les états de Γ parmi les points du plan et en traçant pour tout sommet s et tout $i \in \{0, \ldots, q-1\}$ une arête d'indice i orientée de l'état s vers l'état $\varphi_i(s)$.

5.2. Exemple 1. — Considérons le 2-automate dont les états sont les cinq éléments de l'ensemble $\{*\ ,\ s_\emptyset\ ,\ s_0\ ,\ s_1\ ,\ s_{10}\}$ (le sommet $*$ étant bien sûr l'état initial) et dont l'ensemble des indices coloriant les arêtes orientées de l'état α à l'état ω est donné par la liste

$\alpha \backslash \omega$	$*$	$s_\emptyset$	s_0	s_1	s_{10}
$*$	$\{0\}$	$\{1\}$			
$s_\emptyset$			$\{0\}$	$\{1\}$	
s_0			$\{1\}$	$\{0\}$	
s_1		$\{1\}$			$\{0\}$
s_{10}			$\{0\}$	$\{1\}$	

5.3. Exemple 2. — Soit G un groupe engendré par les éléments d'une suite finie $(g_0, g_1, g_2, \ldots, g_{q-1})$ à valeur dans G avec g_0 appartenant à un sous-groupe donné d'indice fini $H \subset G$.

Considérons le q-automate Γ (aussi appelé le graphe de Schreier de G par rapports aux générateurs $\{g_1, \ldots, g_{q-1}\}$ et par rapport au sous-groupe H) dont les sommets sont les

classes à droite Hg de H. Les fonctions φ_i sont données par $\varphi_i(Hg) = Hgg_i$ et le point base est donné par la classe de H.

Un cas particulièrement célèbre (l'automate associé à la suite de Thue-Morse) est obtenu en prenant la suite $(g_0, g_1) = (\overline{0}, \overline{1})$ dans $G = \mathbf{Z}/2\mathbf{Z}$ avec $H = \{\overline{0}\}$ le sous-groupe trivial de G.

L'exemple 5.3 permet de construire tous les q-automates qui ont la propriété que les applications φ_i sont des bijections. On peut alors prendre pour G le groupe engendré par l'ensemble de ces bijections et pour $H \subset G$ le stabilisateur du point base. En particulier, on peut toujours se ramener au cas où G est un groupe fini dans l'exemple 5.3.

Soit Γ un q-automate. Soit $x_0, x_1, x_2, \ldots \in \{0, \ldots, q-1\}$ la suite des coefficients associée à l'écriture en base q d'un entier $n = \sum x_i q^i \in \mathbf{N}$. Soit $k \in \mathbf{N}$ tel que $x_\ell = 0$ pour tout $\ell > k$. En posant $\gamma_n = \varphi_{x_0} \circ \varphi_{x_1} \circ \varphi_{x_2} \circ \cdots \circ \varphi_{x_k}(*) \in S(\Gamma)$ on obtient une suite $\gamma_0 = *, \gamma_1, \gamma_2, \gamma_3, \ldots$ à valeurs dans les états $S(\Gamma)$ de Γ.

5.4. Définition. — Une suite $a_0, a_1, \ldots$ à valeurs dans un ensemble fini F est *q-automatique* s'il existe un q-automate Γ et une application $\tau : S(\Gamma) \longrightarrow F$ des états de Γ dans F tels que $a_n = \tau(\gamma_n)$ pour tout n (où $\gamma_n \in S(\Gamma)$ est comme ci-dessus).

Remarquons que la modification d'un nombre fini de termes d'une suite automatique ne lui fait pas perdre son automaticité. On peut donc également parler d'automaticité pour une suite de la forme $a_k, a_{k+1}, a_{k+2}, \ldots$

5.5. Exemple. — Soit Γ le 2-automate de l'exemple 5.1. Considérons l'application $\tau(*) = *,\ \tau(s_1) = 1,\ \tau(s_\emptyset) = \tau(s_0) = \sigma(s_{10}) = 0$ de l'ensemble des états $S(\Gamma) \subset \Gamma$ dans $\{*, 0, 1\}$. On obtient ainsi la suite 2-automatique $* \,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1 \cdots$

Soit $p : \{0, \ldots, q-1\}^* \longrightarrow F$ une application du monoïde libre $\{0, \ldots, q-1\}^*$ dans un ensemble fini F.

Associons à un entier $n \geq 1$ un élément $\pi_n \in F$ en posant

$$\pi(n) = p(x_0 x_1 x_2 \cdots x_{k-2} x_{k-1}) \in F$$

où $n = \sum_{i=0}^{k} x_i q^i > 0$ avec $x_i \in \{0, \ldots, q-1\}$ et $x_k > 0$.

5.6. Remarque. — Une suite $\pi_1, \pi_2, \ldots$ d'éléments dans F provient d'une application $p : \{0, \ldots, q-1\}^* \longrightarrow F$ comme ci-dessus si, et seulement si, elle vérifie

$$\pi_n = \pi_{n+q^k} = \pi_{n+2q^k} = \cdots = \pi_{n+(q-1)q^k} \in F$$

pour tout $n, k \in \mathbf{N}$ avec $q^k > n$.

On dira que la fonction $p : \{0,\dots,q-1\}^* \longrightarrow F$ est *automatique* si la suite $p \circ \pi : \mathbf{N} \setminus \{0\} \longrightarrow F$ est q-automatique.

5.7. Proposition. — *Soit $E(\widetilde{G})$ une relation d'équivalence locale engendrée par un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ sur $\mathcal{A}^* = \{0,\dots,q-1\}^*$.*

Alors la projection $p : \mathcal{A}^* \longrightarrow \mathcal{C}$ qui associe à $w \in \mathcal{A}^*$ sa classe d'équivalence $\mathcal{A}^*_w \in \mathcal{C}$ est une fonction automatique.

Preuve. — La version déterministe du pseudo-algorithme 2.2 obtenue en réduisant w toujours le plus à droite possible fournit un q-automate pour la suite $p \circ \pi : \mathbf{N} \setminus \{0\} \longrightarrow \mathcal{C}$. ∎

5.8. Exemple. — On vérifie facilement que la suite 2-automatique construite dans l'exemple 5.5. provient de la relation d'équivalence engendrée par

$$\cdots a0b \cdots \sim \cdots (a+1)(b+1) \cdots$$

(avec $a, b \in \{0,1,\emptyset\}$) sur $\{0,1\}^*$.

5.9. Corollaire. — *Soit $E(\widetilde{G})$ une relation d'équivalence locale engendrée par un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ sur $\mathcal{A}^* = \{0,\dots,q-1\}$.*

Pour toute classe d'équivalence $C \subset \mathcal{A}^*$, il existe un ensemble fini de nombres algébriques $\lambda_j, c_{i_j} \in \mathbf{C}$ avec $i_j \in \mathbf{N}$ tels que

$$\sharp(C \cap \mathcal{A}^n) = \sum_j \sum_{i_j} c_{i_j} n^{i_j} \lambda_j^n .$$

Preuve. — Le nombre $\sharp(C \cap \mathcal{A}^n)$ peut s'exprimer sous la forme $v^t\, A^n u$ où $v, u \in \mathbf{Z}^k$ sont des vecteurs colonnes convenables et où $A \in M_k\mathbf{Z}$). L'entier k désigne le nombre d'états d'un automate associé à la relation d'équivalence $E(\widetilde{G})$. Les nombres algébriques λ_j sont les valeurs propres de A et les facteurs polynomiaux n^{i_j} proviennent de blocs de Jordan. Nous laissons les détails au lecteur. ∎

Le corollaire 3a.6 est une illustration de ce résultat.

5.10. Remarque. — La proposition 5.7 montre que la théorie des relations d'équivalence locales dont le nombre de classes est fini, est un cas particulier de la théorie des suites automatiques.

5.11. Problème. — Caractériser les suites q-automatiques provenant d'une relation d'équivalence avec un nombre fini de classes sur $\{0,\dots,q-1\}^*$ (la remarque 5.6 donne une une condition nécessaire).

6. Stabilisation, mots cycliques

Étant donné un graphe finitaire local $\widetilde{G}$ sur un monoïde libre $\mathcal{A}^*$, les relations d'équivalence locales $\widetilde{E}(\widetilde{G},n)$ (définies juste avant le théorème 2.6) "convergent" vers la relation d'équivalence $E(G)$ quand n tend vers l'infini.

On peut également considérer la relation d'équivalence $\widetilde{E}^{\geq n}(\widetilde{G})$ engendrée par

$$\left\{(x,y)\in\mathcal{A}^{\geq n}\times\mathcal{A}^{\geq n}\mid(x,y)\in\widetilde{G}\right\}$$

sur $\mathcal{A}^{\geq n}$.

6.1. Théorème. — *Il existe un entier M tel que pour tout $r\geq s\geq M$ les deux relations $\widetilde{E}^{\geq r}(\widetilde{G})$ et $\widetilde{E}^{\geq s}(\widetilde{G})$ coïncident sur $\mathcal{A}^{\geq r}$.*

De plus, le nombre de classes des relations d'équivalence $\widetilde{E}^{\geq s}(\widetilde{G})$ est constant et fini pour $s\geq M$.

Idée de la preuve. — Comme le nombre de classes d'équivalence de $E(\widetilde{G})$ est fini, il existe un entier k tel que tout mot de longueur au moins k est aussi équivalent à un mot plus long. Ceci permet d'allonger les éléments d'une chaîne reliant deux mots à condition que tous les mots de la chaîne soient déjà assez longs.

Ce théorème permet d'introduire une relation d'équivalence associée à un graphe finitaire local $\widetilde{G}$ pour les mots cycliques.

Un *mot cyclique* de longueur k est une orbite de $\mathcal{A}^k$ sous l'action du groupe cyclique $\mathbf{Z}/k\mathbf{Z}$ (qui agit en permutant cycliquement les lettres du mot). Un tel mot peut également être considéré comme un mot périodique infini dont on spécifie une période k (qui doit être un multiple de la période minimale).

Je noterai $\overline{w}$ le mot cyclique de longueur $|w|$ associé au mot $w\in\mathcal{A}^*$ et je noterai $\mathcal{A}_{\text{cyc}}$ l'ensemble des mots cycliques.

Étant donné un graphe finitaire $\widetilde{G}\in\mathcal{A}^*\times\mathcal{A}^*$, on obtient une relation d'équivalence $E_{\text{c}}^{\geq n}\subset\mathcal{A}_{\text{cyc}}{\geq}\ n\times\mathcal{A}_{\text{cyc}}^{\geq n}$ en considérant

$$\left\{(\overline{xuy},\overline{\alpha(x)u\omega(y)})\in\mathcal{A}_{\text{cyc}}^{\geq n}\times\mathcal{A}_{\text{cyc}}^{\geq n}\mid x\in\mathcal{A}^{\geq|\alpha|},\ y\in\mathcal{A}^{\geq|\omega|}\text{ et }(xuy,\alpha(x)v\omega(y))\in\tilde{G}\right\}.$$

6.2. Théorème. — *Il existe un entier M tel que pour tout $r \geq s \geq M$ les deux relations $E_{\widetilde{c}}^{\geq r}(\widetilde{G})$ et $E_{\widetilde{c}}^{\geq s}(\widetilde{G})$ coïncident sur les mots cycliques $\mathcal{A}_{\mathrm{cyc}}^{\geq r}$ de longueur au moins r.*

De plus, le nombre de classes des relations d'équivalence $E_{\mathrm{cyc}}^{\geq s}(\widetilde{G})$ est constant et fini pour $s \geq M$.

La preuve est analogue à la preuve du cas précédent.

Ainsi les valeurs des longueurs primitives considérées à la section 3b (voir assertion *(ii)* de la proposition 3b.5) sont liées aux classes d'équivalence "stabilisées" des suites cycliques. En particulier, la relation d'équivalence stabilisée sur les mots binaires cycliques assez longs engendrée par $\cdots a0b\cdots \sim \cdots(a+1)(b+1)\cdots$ doit avoir au moins trois classes.

7. Conclusion

Beaucoup de problèmes concernant les relations d'équivalence isotropes et locales ont un fort goût algorithmique.

Ainsi il n'est pas difficile de concevoir un algorithme, qui étant donné un ensemble fini $\mathcal{G}$ de graphes isotropes, "décide" si la relation d'équivalence $E(\mathcal{G})$ engendrée par $\mathcal{G}$ possède un nombre fini de classes (cet algorithme continuera cependant infiniment si la réponse est non et l'exemple 1.4 montre qu'on ne pourra pas toujours déterminer si l'algorithme s'arrête).

En cas de réponse positive à cette question, la détermination d'un graphe finitaire $\widetilde{G} \subset \mathcal{A}^* \times \mathcal{A}^*$ est complètement algorithmique de même que la détermination du nombre exact de classes d'équivalence si $\widetilde{G}$ est de plus local.

Je pense que les sections 3, 3a, 3b et 4 contiennent les résultats les plus intéressants de ce papier.

Le contenu des sections 1 et 2 est sans doute bien connu des spécialistes des systèmes de réécriture et a été inclus pour la commodité du lecteur (ainsi que par ignorance de la littérature de la part de l'auteur).

Je remercie Jean-Paul Allouche pour ses suggestions et remarques judicieuses.

Bibliographie

[A] J.-P. Allouche. — *Automates finis en théorie des nombres*, Exposition. Math. **5** (1987), 239–266.

[Ba] R. Bacher. — *Curvature flows of maximal integral triangulations*, Prépublication de l'Institut Fourier n° 450, Grenoble, 1999.

[Bou] N. Bourbaki. — *Théorie des ensembles*, Hermann (Paris), 1970.

[C] A. Cobham. — *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192.

[DMP] F. M. Dekking, M. Mendès France and A. van der Poorten. — *Folds!*, Math. Intelligencer **4** (1982), 130–138, 173–181, 190–195.

[E] S. Eilenberg. — *Automata, Languages and Machines*, Academic Press (New York and London), 1974.

[Ha] M. Hazewinkel. — *Introductory Recommendations for the Study of Hopf Algebras in Mathematics and Physics*, CWI-Quarterly **4**, (1) (1991), 3–26.

[Ho] J. Howie. — *Automata and languages*, (Oxford), 1991.

– ◇ –

Roland BACHER
Université de Grenoble I
Institut Fourier
Laboratoire de Mathématiques
UMR 5582 CNRS-UJF
B.P. 74
38402 ST MARTIN D'HÈRES Cedex (France)
e-mail : Roland.Bacher@ujf-grenoble.fr

(22 mars 1999)